

PATENT ABSTRACTS OF JAPAN

(1)Publication number : 2002-278930

(43)Date of publication of application : 27.09.2002

(51)IntCl

G06F 15/00

G06F 12/00

G06F 17/30

(21)Application number : 2001-079821

(71)Applicant : TOYOTA MOTOR CORP
TOYOTA DIGITAL CRUISE NC

(22)Date of filing : 21.03.2001

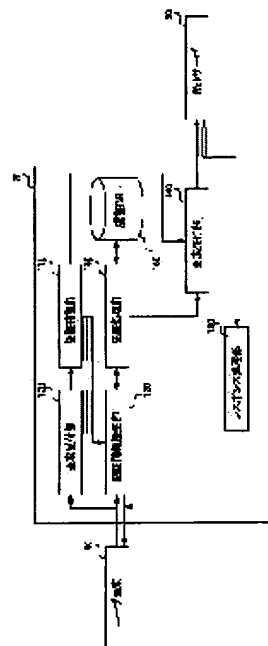
(72)Inventor : SADAKATA AKIRA
TAKANO MASATOSHI
TAKASHIMA NAOKA
TSUTSUMI YOSHINAGA

(54) AUTHENTICATION SYSTEM AND AUTHENTICATION SERVER

(57)Abstract:

PROBLEM TO BE SOLVED: To provide technology for reducing loads by an authentication processing when a user reads a plurality of URLs.

SOLUTION: This system for transmitting the URL requiring user authentication to the user is provided with an access reception means for receiving the request of accessing a desired web page from the user, a user authentication means for authenticating the user requesting access, an authentication database storing a plurality of web pages which the user can access by authentication, and a web transmission means for transmitting the desired web page from a plurality of web pages to a terminal which the user uses to the user who is once authenticated.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-278930

(P2002-278930A)

(43) 公開日 平成14年9月27日 (2002.9.27)

(51) Int.Cl. ⁷	識別記号	F I	テーマコード* (参考)
G 0 6 F 15/00	3 3 0	G 0 6 F 15/00	3 3 0 B 5 B 0 7 5
12/00	5 3 7	12/00	5 3 7 D 5 B 0 8 2
17/30	1 1 0	17/30	1 1 0 F 5 B 0 8 5
	1 2 0		1 2 0 B

審査請求 未請求 請求項の数 5 O L (全 9 頁)

(21) 出願番号 特願2001-79821(P2001-79821)

(22) 出願日 平成13年3月21日 (2001.3.21)

(71) 出願人 000003207

トヨタ自動車株式会社

愛知県豊田市トヨタ町1番地

(71) 出願人 501111452

株式会社トヨタデジタルクルーズ

愛知県名古屋市中区錦2丁目15番5号 豊島ビル14階

(72) 発明者 定方 暁

愛知県豊田市トヨタ町1番地 トヨタ自動車株式会社内

(74) 代理人 100075258

弁理士 吉田 研二 (外2名)

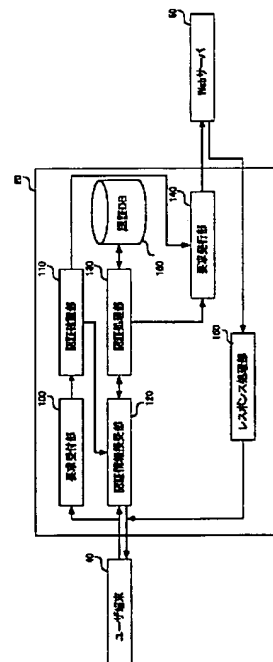
最終頁に続く

(54) 【発明の名称】 認証システム、および認証サーバ

(57) 【要約】

【課題】 従来、ユーザは、サーバ内の特定のアプリケーション (URL) へアクセスするためには、URLごとに、アクセス認証のために、ユーザIDとパスワードを入力する必要があった。したがって、アクセスしたいURLの数が多くなるにつれて、認証に必要な入力による負担が増加し、作業効率の低下をまねいていた。

【解決手段】 本発明は、ユーザ認証を必要とするURLをユーザに送信する装置であって、ユーザから所望のウェブページへのアクセスの要求を受け付けるアクセス受付手段と、アクセスを要求したユーザを認証するユーザ認証手段と、ユーザが認証によりアクセス可能な複数のウェブページを格納する認証データベースと、一旦認証されたユーザに対して、複数のウェブページの中から所望のウェブページをユーザが利用する端末に送信するウェブ送信手段と、を備える。



【特許請求の範囲】

【請求項1】 ユーザ認証を必要とするウェブページをユーザに送信する装置であって、ユーザから所望のウェブページへのアクセスの要求を受け付けるアクセス受付手段と、

アクセスを要求したユーザを認証するユーザ認証手段と、

ユーザが認証によりアクセス可能な複数のウェブページを格納する認証データベースと、

一旦認証されたユーザに対して、複数のウェブページの中から所望のウェブページをユーザが利用する端末に送信するウェブ送信手段と、

を備えることを特徴とする認証サーバ。

【請求項2】 認証されたユーザによるウェブページへのアクセスを、ユーザが認証された後、所定の時間内に制限する手段をさらに備えることを特徴とする請求項1に記載の認証サーバ。

【請求項3】 ユーザ認証手段は、ユーザが用いる端末を識別する情報を、ユーザ認証に用いることを特徴とする請求項1に記載の認証サーバ。

【請求項4】 ユーザがアクセス可能な複数のウェブページの一覧、および各ウェブページにアクセス可能な有効時間の残り時間をユーザの端末に送信する手段をさらに備えることを特徴とする請求項2に記載の認証サーバ。

【請求項5】 ユーザ認証を必要とするウェブページをユーザに送信するシステムであって、ユーザから所望のウェブページへのアクセスの要求を受け付けるアクセス受付手段と、

アクセスを要求したユーザを認証するユーザ認証手段と、

ユーザが認証によりアクセス可能な複数のウェブページを格納する認証データベースと、

一旦認証されたユーザに対して、複数のウェブページの中から所望のウェブページをユーザが利用する端末に送信するウェブ送信手段と、

を備えることを特徴とする認証システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、認証システム、および認証サーバに関する。特に本発明は、ユーザが複数のURLを閲覧する際に、認証処理による負担を少なくする技術に関する。

【0002】

【従来の技術】近年、ネットワークの普及により、外出先からでも、インターネットを介して、企業が所有する社内LANに接続されたサーバにアクセスすることにより、サーバが有するアプリケーション、ファイル、メールおよびその他のデータを実行、または閲覧することができるようになった。ただし、社内LANのサーバへのアクセ

スは、セキュリティを考慮して、アプリケーションごとに、IDとパスワードが設定されており、社内LAN内の所望のアプリケーションおよびファイルを実行する前に、IDとパスワードによるユーザの認証が行われている。

【0003】たとえば、特開2000-83285号公報は、携帯電話固有のIDを用いてその加入者を特定し、加入者別の個別サービスを開示する。

【0004】また、特開平11-341151号公報は、ダイヤルアップ認証を行う際に、発信電話番号を用いて許可された発信電話番号のみにログイン認証を行う技術を開示する。

【0005】

【発明が解決しようとする課題】従来、ユーザは、サーバ内の特定のアプリケーション（URL）へアクセスするためには、URLごとに、アクセス認証のために、ユーザIDとパスワードを入力する必要があった。したがって、アクセスしたいURLの数が多くなるにつれて、認証に必要な入力による負担が増加し、作業効率の低下をまねいていた。

20 【0006】ユーザの認証に関しては、ユーザIDとパスワードによる認証では、パスワードが漏洩した場合どこからでもアクセスされてしまうという欠点があった。

【0007】また、認証サーバでの認証がユーザが用いる携帯電話などに固有のIDだけの場合、企業によっては、携帯電話自体が貸し出し制のところもあるため、個人の特定には至らない。このため、紛失や盗難にあったときにアプリケーションに不正にアクセスされてしまう。

30 【0008】ダイヤルアップ認証を行う際に、発信電話番号を用いて認証を行う場合には、リモートログインする際に発信者側の端末（電話機）は、発信者番号通知の設定をしていなければならない。

【0009】そこで本発明は、上記の課題を解決することのできる認証システム、および認証サーバを提供することを目的とする。

【0010】

【課題を解決するための手段】本発明は、ユーザ認証を必要とするウェブページをユーザに送信する装置であって、ユーザから所望のウェブページへのアクセスの要求を受け付けるアクセス受付手段と、アクセスを要求したユーザを認証するユーザ認証手段と、ユーザが認証によりアクセス可能な複数のウェブページを格納する認証データベースと、一旦認証されたユーザに対して、複数のウェブページの中から所望のウェブページをユーザが利用する端末に送信するウェブ送信手段と、を備える。

【0011】本発明は、認証されたユーザによるウェブページへのアクセスを、ユーザが認証された後、所定の時間内に制限する手段をさらに備えてもよい。

50 【0012】本発明のユーザ認証手段は、ユーザが用いる端末を識別する情報を、ユーザ認証に用いてもよい。

【0013】本発明は、ユーザがアクセス可能な複数のウェブページの一覧、および各ウェブページにアクセス可能な有効時間の残り時間をユーザの端末に送信する手段をさらに備えてもよい。

【0014】また、本発明は、ユーザ認証を必要とするウェブページをユーザに送信するシステムであって、ユーザから所望のウェブページへのアクセスの要求を受け付けるアクセス受付手段と、アクセスを要求したユーザを認証するユーザ認証手段と、ユーザが認証によりアクセス可能な複数のウェブページを格納する認証データベースと、一旦認証されたユーザに対して、複数のウェブページの中から所望のウェブページをユーザが利用する端末に送信するウェブ送信手段と、を備える。

【0015】

【発明の実施の形態】以下、発明の実施の形態を通じて本発明を説明する。

【0016】図1は、本実施形態に係るユーザ認証システム10の全体像を示す概略図である。本実施例は、ユーザが外出先から、会社のLANに接続されたアプリケーション、文書、データ等にアクセスする場合に好適な例である。ユーザ端末40と、認証サーバ20とは、インターネット30を介して接続されている。ユーザ端末40の具体例としては、携帯電話、PHS、ノートパソコン、PDA(Personal Digital Assistant)などがある。認証サーバ20は、各企業の社内LAN内のWebサーバ50と接続されている。Webサーバ50には、アプリケーションなどが格納されている。このアプリケーションには、ユーザごとにユーザID、およびパスワードが設定されている。

【0017】図2は、認証サーバ20の構成を示すブロック図である。認証サーバ20は、要求受付部100、認証確認部110、認証情報授受部120、認証処理部130、要求発行部140、レスポンス処理部150、および認証データベース160を含む。

【0018】要求受付部100は、ユーザ端末40からユーザがアクセスしたいURLの要求を受け付ける。このとき、要求受付部100は、ユーザ端末40に認証サーバ20によって発行された認証情報がある場合には、認証情報も受け付ける。認証情報としては、たとえば、Cookieが好適な例である。認証情報については、後述する。また、要求受付部100は、ユーザが使用するユーザ端末40に固有な端末IDも受け付けることができる。

【0019】認証確認部110は、URLを要求したユーザが認証済みか否かを認証情報を使って調べる。ここで、認証情報の具体例を図3に示す。認証情報には、認証サーバ20がユーザを識別するためのユーザ識別番号に、前回認証された日時、および、認証されたURLが対応付けられている。認証確認部110は、ユーザが要求したURLに認証の有効期間が設定されている場合には、前回認証された日時と現在時刻とから、有効期間が切れ

ていないか否かを判断する。

【0020】次に、図2に戻り、認証情報授受部120は、ユーザ端末40に、要求したURLのアクセスに必要なユーザIDおよびパスワードを要求するとともに、ユーザ端末40からのユーザIDおよびパスワードの入力を受け付ける。

【0021】認証処理部130は、受け付けたユーザID、パスワード、および機器IDについて、後述する認証データベース160を用いて認証処理を行う。認証処理の結果は、ログファイルに履歴として記録される。

【0022】要求発行部140は、ユーザ端末40から要求されたURLを、ユーザに代わってWebサーバ50に要求する。

【0023】レスポンス処理部150は、Webサーバ50から所定のコンテンツを受け取った後、ユーザ端末40に送る。

【0024】認証データベース160は、認証によってアクセス可能となるURLに対応付けて、ユーザID、パスワード、および機器IDを格納する。図4～6に、認証データベース160が含むテーブルの例を示す。

【0025】図4は、各URLとユーザID等とを関連付けるURLテーブル200の例を示す。URLテーブル200は、各URLのアドレスに、認証によりアクセスが許可されるユーザのユーザID、パスワード、ユーザが用いる機器の機器ID、および認証サーバ20がユーザを識別するためのユーザ識別情報を対応づけて格納する。URLテーブル200は、ユーザが新たに、所定のURLへのアクセスを許可された場合、その他変更などが生じた場合にはその都度更新される。

【0026】図5は、各URLと認証後の有効期間とを連付ける有効期間テーブル210の例を示す。有効期間テーブル210は、各URLのアドレスに、各URLに設定された認証の有効期間を関連付けて格納する。

【0027】図6は、各ユーザを識別するユーザ識別番号と、各ユーザにURL設定されたユーザIDとを関連付けるユーザテーブル220の例を示す。ユーザテーブル220は、認証サーバ20が各ユーザを識別するためのユーザ識別番号に対応づけて、各URLに設定されたユーザIDを設定する。このテーブルにより、各ユーザが認証によりアクセス可能なURLが一覧できる。

【0028】[動作]図7は、本実施形態に係るユーザ認証システム10によって、ユーザが所望のURLを要求してから、閲覧するまでのシーケンスチャートである。このシーケンスチャートを用いて、ユーザ認証システム10の動作を説明する。

【0029】まず、ユーザは、ユーザ端末40を用いて認証サーバ20にアクセスしたいURLを要求する(S10)。その際に、後述する認証情報、および機器IDが認証サーバ20に送られる。認証サーバ20は、送られた認証情報を用いて、URLを要求したユーザが認証済みで

あるか、および、要求されたURLがユーザテーブル220に記録されているかを調べる(S20)。

【0030】ユーザが認証済みで、かつ、要求されたURLがユーザテーブル220に記録されている場合には、認証サーバ20は、ユーザの要求をWebサーバ50に発行する(S70)。Webサーバ50は、認証サーバ20からの要求に応じてコンテンツを認証サーバ20に返す(S80)。認証サーバ20は、Webサーバ50から受け取ったコンテンツを、ユーザ端末40に送る(S90)。

【0031】一方、ユーザが認証済みでない場合、または、要求されたURLがユーザテーブル220に記録されていない場合には、認証サーバ20は、ユーザ端末40にユーザID、およびパスワード、またはURLを要求する(S30)。認証サーバ20からの要求に応じて、ユーザ端末40からユーザIDおよびパスワード、またはURLが入力される(S40)。このとき、ユーザ端末40を識別する機器IDが認証サーバ20に送られる。入力されたユーザID、パスワード、機器ID、およびアクセス要求があったURLについて、認証データベース160を用いて認証処理が行われる(S50)。入力されたユーザID、およびパスワード等が認証されない場合には、再度ユーザID、パスワード等を要求する(S30)。入力されたユーザID、およびパスワード等が認証された場合には、ユーザ端末40に認証情報が発行される(S60)。認証情報には、ユーザが認証されたことを示す情報、認証の有効期限に関する情報などが含まれる。また、ログファイルに認証に関する情報が履歴として記録される。認証サーバ20は、次に、ユーザの要求をWebサーバ50に発行する(S70)。Webサーバ50は、認証サーバ20からの要求に応じてコンテンツを認証サーバ20に返す(S80)。認証サーバ20は、Webサーバ50から受け取ったコンテンツを、ユーザ端末40に送る(S90)。

【0032】ユーザは、一旦認証されると、認証の有効期限内であれば、次にユーザにアクセス権が設定されたURLを要求するときには、再度ユーザIDやパスワードを入力する必要がないので、本来ならば認証が必要なURLを迅速に閲覧することができる。

【0033】また、認証処理においては、ユーザIDとパスワードに加えて、ユーザが使用する端末の機器IDも照合しているので、ユーザIDとパスワードが不正に使用された場合でも、使用する端末が異なれば、アクセスを拒否することができる。

【0034】[画面表示]次に、図8～10を用いて、ユーザに表示される画面について説明する。

【0035】図8は、ユーザがアクセスしたいURLを入力するときの入力画面300の例を示す。ユーザが既に他のURLなどで認証済みの場合には、ユーザは、認証処理をすることなく、入力したURLを閲覧することができ

る。認証の有効期限が切れているなどの理由により、ユーザのアクセスが拒否された場合には、図9のID入力画面310が表示される。ここで、ユーザは、入力したURLに設定されたユーザIDおよびパスワードを入力する。ユーザIDおよびパスワードが認証されると、ユーザは所望のURLを閲覧することができる。

【0036】ユーザは、一旦認証されると、認証サーバ20に登録された他のURLへのアクセスも所定期間の間許可される。これにより、ユーザはURLごとに、ユーザIDおよびパスワードを入力するという手間を省くことができる。

【0037】また、認証サーバ20からは、図10に示すように、ユーザがアクセス可能なURLのリストが提供される。ユーザは、アクセス可能と表示されたURLをクリックすることにより、所望のURLを閲覧することができ、各URLを手入力する場合に比べて、作業効率が大幅に改善される。また、各URLには、アクセス可能な残り時間が表示される。これにより、ユーザは、残りアクセス可能時間が予め分かるので、URLにアクセス中に突然アクセスが切られるという事態を未然に防止することができる。

【0038】また、複数の社内LANを含む企業間イントラネットのゲートウェイに、認証サーバ20を用いることにより、企業間イントラネット内に設置された、Webサーバ50への不正なアクセスを未然に防止することができる。このため、社内LANへの不正なアクセスによる、企業間イントラネット内のトラフィックの増加を防止することができる。また、この企業間イントラネットに接続している企業は、社内LANにアクセスするための専用線を別途敷設することなく、携帯電話等を用いて外出先から社内LANへのセキュアなアクセスが可能となる。

【0039】さらに、従来は、アプリケーション(Webサーバ50)側で個別の認証の仕組みを設ける必要があったが、認証サーバ20に認証の仕組みを持つことで、Webサーバ50側には許可された端末やユーザのアクセスのみとなり、アプリケーションの負荷軽減にもなる。

【0040】以上、本発明を実施の形態を用いて説明したが、本発明の技術的範囲は上記実施の形態に記載の範囲には限定されない。上記実施の形態に、多様な変更又は改良を加えることができる。その様な変更又は改良を加えた形態も本発明の技術的範囲に含まれ得ることが、特許請求の範囲の記載から明らかである。

【0041】

【発明の効果】上記説明から明らかなように、本発明によれば、ユーザは、認証が必要なURLに一旦アクセスすることにより、本来なら認証が必要な他のURLに、認証処理の手間なしにアクセスすることができる。

【図面の簡単な説明】

50 【図1】 本実施形態に係るユーザ認証システム10の

全体像を示す概略図である。

【図2】 認証サーバ20の構成を示すブロック図である。

【図3】 ユーザ端末40と認証サーバ20とでやり取りされる、認証情報の例を示す図である。

【図4】 各URLとユーザID等とを関連付けるURLテーブル200の例を示す図である。

【図5】 各URLと認証後の有効期間とを連付ける有効期間テーブル210の例を示す図である。

【図6】 ユーザを識別するユーザ識別番号と、各ユーザにURL設定されたユーザIDとを関連付けるユーザテーブル220の例を示す図である。

【図7】 本実施形態に係るユーザ認証システム10によって、ユーザが所望のURLを要求してから、閲覧する *

*までのシーケンスチャートである。

【図8】 ユーザがアクセスしたいURLを入力するときの入力画面300の例を示す図である。

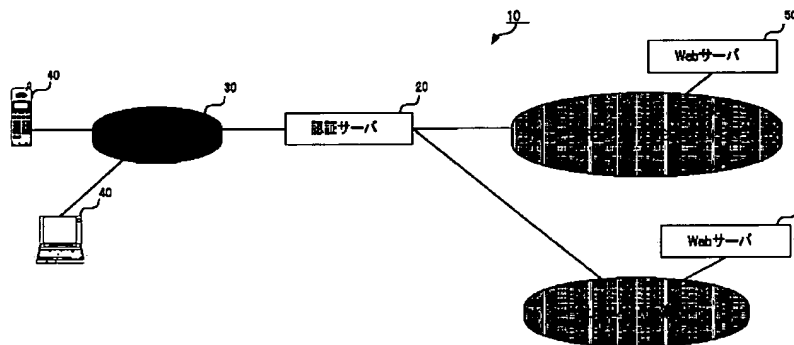
【図9】 ID入力画面310の例を示す図である。

【図10】 ユーザがアクセス可能なURLのリストを表示するURLリスト画面320の例を示す図である。

【符号の説明】

10 ユーザ認証システム、20 認証サーバ、30 インターネット、40 ユーザ端末、50 Webサーバ、100 要求受付部、110 認証確認部、120 認証情報授受部、130 認証処理部、140 要求発行部、150 レスポンス処理部、160 認証データベース。

【図1】



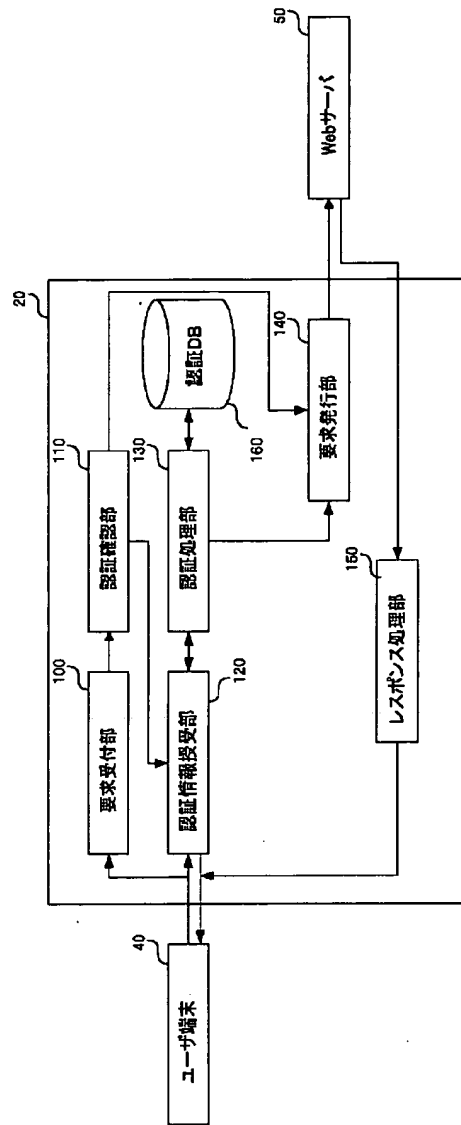
【図3】

ユーザ識別番号	認証日時	認証されたURL
1	2001/3/14 15:00	http://www.xxx.ne.jp/application01/

【図4】

対象URL	許可ユーザID	パスワード	機器ID	ユーザ識別番号
http://www.xxx.ne.jp/application01/	adk001a	xxxxxxxx	abc001	1
http://www.xxx.ne.jp/application01/	adk002a	xxxxxxxx	abc002	2
...
http://www.xxx.ne.jp/application02/	xyz001x	xxxxxxxx	abc001	1
http://www.xxx.ne.jp/application02/	adk003a	xxxxxxxx	abc003	3
...

【図2】



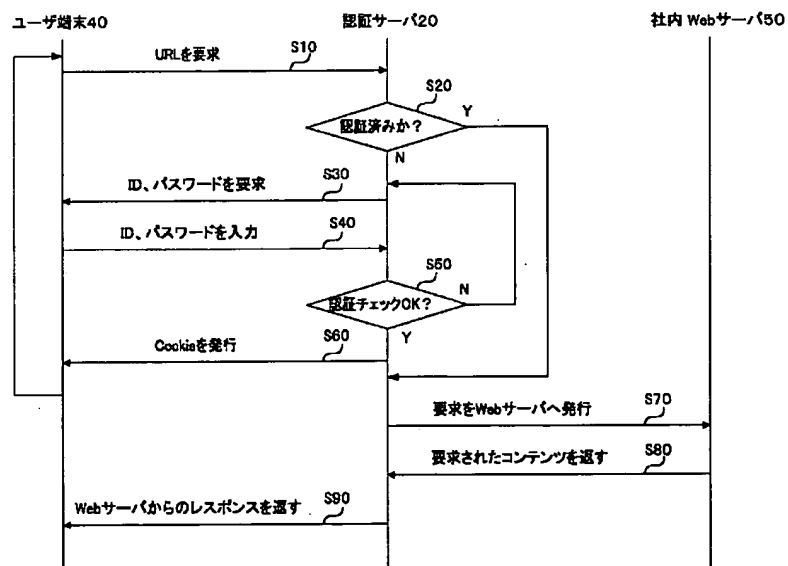
【図5】

対象URL	認証有効期間
http://www.xxx.ne.jp/application01/	5時間
http://www.xxx.ne.jp/application02/	10時間
http://www.xxx.ne.jp/application03/	3時間
...	...

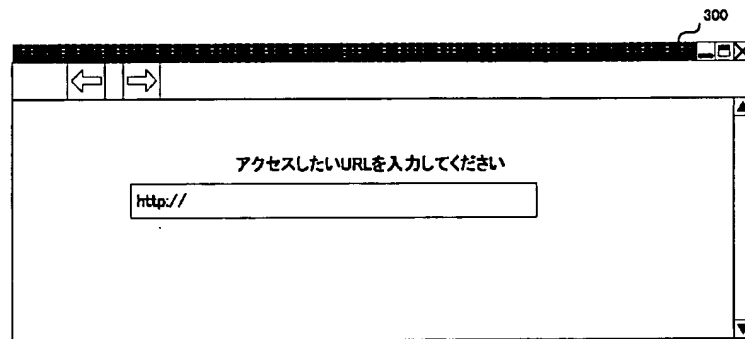
【図6】

ユーザ識別番号	ユーザID
1	adk001a
1	xyz001x
...	...

【図7】



【図8】



300

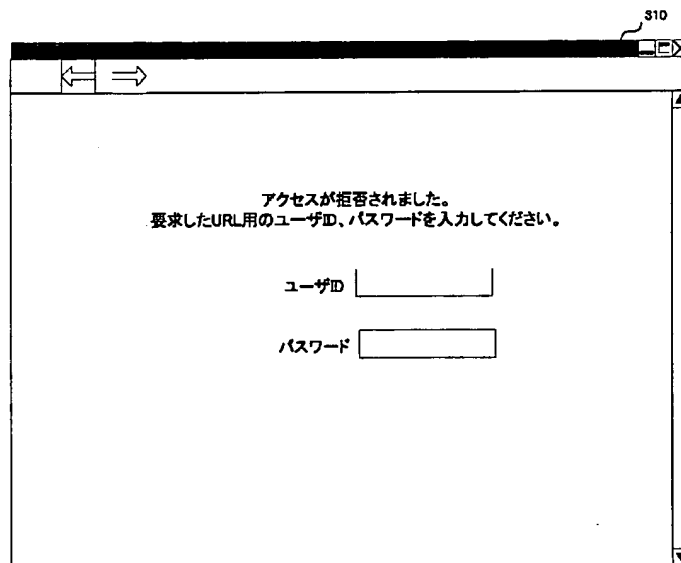
← →

アクセスしたいURLを入力してください

http://

This diagram shows a web browser window labeled 300. The window has a title bar with standard OS controls (minimize, maximize, close) and a navigation bar with back and forward buttons. The main content area displays the text "アクセスしたいURLを入力してください" (Please enter the URL you want to access). Below this text is a text input field containing the text "http://".

【図9】



310

← →

アクセスが拒否されました。
要求したURL用のユーザID、パスワードを入力してください。

ユーザID

パスワード

This diagram shows a web browser window labeled 310. The window has a title bar with standard OS controls (minimize, maximize, close) and a navigation bar with back and forward buttons. The main content area displays the text "アクセスが拒否されました。" (Access is denied.) followed by "要求したURL用のユーザID、パスワードを入力してください。" (Please enter the user ID and password for the requested URL). Below this text are two input fields: one labeled "ユーザID" (User ID) and another labeled "パスワード" (Password).